COMPLIANCE AND CONTROL AUDIT REPORT

Juvenile Justice Authority Information Systems: Reviewing the Authority's Management of Those Systems

A Report to the Legislative Post Audit Committee
By the Legislative Division of Post Audit
State of Kansas
March 2003

03-G

Legislative Post Audit Committee
Legislative Division of Post Audit

The Legislative Post Audit Committee and its audit agency, the Legislative Division of Post Audit, are the audit arm of Kansas government. The programs and activities of State government now cost about $9 billion a year. As legislators and administrators try increasingly to allocate tax dollars effectively and make government work more efficiently, they need information to evaluate the work of government agencies. The audit work performed by Legislative Post Audit helps provide that information.

We conduct our audit work in accordance with applicable government auditing standards set forth by the U. S. General Accounting Office. These standards pertain to the auditor's professional qualifications, the quality of the audit work, and the characteristics of professional and meaningful reports. These audit standards have been endorsed by the American Institute of Certified Public Accountants and adopted by the Legislative Post Audit Committee.

The Legislative Post Audit Committee is a bipartisan committee comprising five senators and five representatives. Of the Senate members, three are appointed by the President of the Senate and two areappointed by the Senate Minority Leader. Of the representatives, three are appointed by the Speaker of the House and two are appointed by the House Minority Leader.

As part of its audit responsibilities, the Division is charged with meeting the requirements of the Legislative Post Audit Act which address audits of financial matters. Those requirements call for two major types of audit work.

First, the Act requires an annual audit of the State's financial statements. Those statements, prepared by the Department of Administration's Division of Accounts and Reports, are audited by a certified public accounting firm under contract with the Legislative Division of Post Audit. The firm is selected by the Contract Audit Committee, which comprises three members of the Legislative Post Audit Committee (including the Chairman and Vice-Chairman), the Secretary of Administration, and the Legislative Post Auditor. This audit work also meets the State's audit responsibilities under the federal Single Audit Act.

Second, the Act provides for a regular audit presence in every State agency by requiring that audit work be conducted at each agency at least once every three years. Audit work done in addition to the annual financial statement audit focuses on compliance with legal and procedural requirements and on the adequacy of the audited agency's internal control procedures. These compliance and control audits are conducted by the Division's staff under the direction of the Legislative Post Audit Committee.

LEGISLATIVE POST AUDIT COMMITTEE

Representative John Edmonds, Chair
Representative Tom Burroughs
Representative Bill McCreary
Representative Frank Miller
Representative Dan Thimesch

Senator Derek Schmidt, Vice-Chair
Senator Bill Bunten
Senator Anthony Hensley
Senator Dave Kerr
Senator Chris Steineger

LEGISLATIVE DIVISION OF POST AUDIT

800 SW Jackson
Suite 1200
Topeka, Kansas 66612-2212
Telephone (785) 296-3792
FAX (785) 296-4482
E-mail: LPA@lpa.state.ks.us
Website: http://kslegislature.org/postaudit
Barbara J. Hinton, Legislative Post Auditor

The Legislative Division of Post Audit supports full access to the services of State government for all citizens. Upon request, Legislative Post Audit can provide its audit reports in large print, audio, or other appropriate alternative format to accommodate persons with visual impairments. Persons with hearing or speech disabilities may reach us through the Kansas Relay Center at 1-800-766-3777. Our office hours are 8:00 a.m. to 5:00 p.m., Monday through Friday.

LEGISLATURE OF KANSAS

LEGISLATIVE DIVISION OF POST AUDIT

800 SOUTHWEST JACKSON STREET, SUITE 1200
TOPEKA, KANSAS 66612-2212
TELEPHONE (785) 296-3792
FAX (785) 296-4482
E-MAIL: lpa@lpa.state.ks.us

March 14, 2003

To: Members, Legislative Post Audit Committee

Representative John Edmonds, Chair
Representative Tom Burroughs
Representative Bill McCreary
Representative Frank Miller
Representative Dan Thimesch

Senator Derek Schmidt, Vice-Chair
Senator Bill Bunten
Senator Anthony Hensley
Senator Dave Kerr
Senator Chris Steineger

This report contains the findings, conclusions, and recommendations from our completed performance audit, *Juvenile Justice Authority Information Systems: Reviewing the Authority's Management of Those Systems*.

The report includes several recommendations for the Authority. We would be happy to discuss these recommendations or any other items in the report with any legislative committees, individual legislators, or other State officials.

Barbara J Hinton

Barbara J. Hinton
Legislative Post Auditor

EXECUTIVE SUMMARY

LEGISLATIVE DIVISION OF POST AUDIT

Overview of the Juvenile Justice Authority's Information System Function

The Juvenile Justice Authority was created in 1997 to coordinate and administer custody and programs for juvenile offenders in State custody. The Authority is developing a comprehensive Statewide information system for juvenile offender data that can be accessed by various agencies and programs that deal with juveniles. The system will consist of the several major applications, most of which will contain sensitive confidential information about juveniles in the Authority's custody and supervision. Most of these applications will be web-based. .... page 2

Currently, the Authority has 7 information systems staff in the central office, and 4 staff at the juvenile facilities. Two of those central office staff have significant security responsibilities. In addition, database security is handled by the database administrator.

Question 1: How Well Is the Juvenile Justice Authority Managing the Security of Its Information Systems?

***Security planning allows an organization to identify its vulnerabilities and focus resources where they are most needed**. Without good security planning, there's an increased risk agencies will have poor security over their information systems, or will focus their security resources in the wrong directions. Leading organizations use a cycle of planning activity consisting of analyzing risks, developing policies to address the risks, and monitoring the effectiveness of those policies.* .... page 4

***The Authority has never done a formal security risk assessment**. An organized assessment of risks is the base from which security policies and plans should flow. The Authority has no policy requiring periodic risk assessments, and has never done a formal assessment. As a result, Authority staff don't know if they are missing important vulnerable areas.* .... page 5

The Authority has inadequate security polices or practices in several important areas. *The Authority had many of the policies we were looking for. However, we found several important policies to be missing. For example, we noted the Authority:* .... page 5

- *was missing policies having to do with incident response and reporting*
- *lacked policies on audit trails*
- *had no written policies on passwords, and some of its password practices are weak*

- *didn't address enforcement issues in its security policies*
- *lacked documentation for how some of its servers are configured*

Since our audit began, the Authority has addressed a number of these weaknesses.

The Authority does little active monitoring of its security function's effectiveness*. The only way for upper-level management to ensure that security policies are carried out and remain effective is to monitor those policies and controls. The Authority has no policies in this area, and does little active monitoring of how well its security function is working to safeguard its systems and information. (It does actively monitor certain areas such as the firewall and virus protection software.)* .... page 7

Conclusion .... page 7

Recommendations .... page 8

Question 2: How Well Is the Authority Limiting Unauthorized Access To Its Information System Resources?

Access controls are the core of an organization's security, determining who gets into a system and what they're allowed to do once they're there. *Access controls protect computer systems and system data from unauthorized modification, disclosure, loss, or impairment. They are designed to limit access only to those people who are authorized, and to limit authorized users only to the minimum level of access they need to do their jobs.* .... page 9

The Authority has some access control elements that provide very strong security for agency data. *For some of its systems, the Authority goes beyond ordinary password controls and uses a method of authenticating users that's far more secure. The Authority also uses an intrusion detection system that monitors all traffic attempting to come into the Authority's network. Few State agencies have such systems at this time.* .... page 9

Weaknesses in some of the access controls in the authority's central office network increased its vulnerability. *The Authority generally had good network controls—it made good use of tools that simplify some of the possible complexity in network security, and was good at authorizing users' access only to those resources they needed to do their work. However, we did note the following significant weaknesses:* .... page 10

- *The Authority had some weak network passwords requirements, allowing us to break a total of 70% of the passwords in 8 hours, including some administrative passwords*

- *The security “patches” for the Authority’s web-based Juvenile Justice Information System weren’t current*
- *Although the Authority had a policy to disable accounts immediately after an employee leaves, we found that 2 of 10 employees who recently left the agency still had active accounts*
- *The intruder lockout function wasn’t turned on for the central office and for one of the juvenile facilities*
- *The Authority had set its firewall to give users in 2 segments of the network more access than they needed to other parts of the network*

The Authority’s method of assigning access to data could be improved. *The Authority has a system to make sure new users get assigned access only to those files they need to do their jobs. We found the following problems with the system:*

.... page 11

- *Information systems staff don’t retain the original forms used to assign access privileges*
- *Information systems staff don’t periodically review employees’ access privileges*
- *The general network diagram the Authority publishes in its annual report provides more information than is prudent*
- *The Authority requires users of the Juvenile Justice Information System to get criminal background checks, but has given them access even when they didn’t pass*

Conclusion

.... page 11

Recommendations

.... page 12

Question 3: Is the Authority Adequately Managing Changes to Its Critical Software?

Because of the dynamic nature of computer software, it’s important to have a well organized system to manage the process of making changes. *Large and complex computer programs are constantly in flux. As a result, computer programs remain works in progress long after they are put into daily use. However, if the activities involved in changing software aren’t closely organized and managed, the software can quickly become unreliable.*

.... page 13

The Authority’s change control process had many of the elements of a good system, but several improvements are needed. *We noted the Authority was missing change control processes in the following areas:*

.... page 13

- *it doesn’t have a formal “configuration management process” that would document changes to the network and server software*

- *it doesn't require the information technology manager to approve in writing the incorporation of software changes into the production software*
- *it doesn't use the change control process for tracking computer bugs*

Finally, we noted the Authority needs to develop a better tracking form and to require management to document completion of important steps.

Recommendation .... page 14

Question 4: Has the Authority Done Adequate Disaster-Recovery Planning To Minimize The Loss of Computer Operations In Case of a Disaster?

An organization needs good business continuity planning in order to quickly recover critical operations after a disaster. *Business continuity planning addresses an organization's ability to continue functioning when normal operations are disrupted. By necessity, it includes planning for contingencies and is focused on the information system functions that are the most critical to continue agency operations.* .... page 15

The Authority lacks the tools necessary to recover operations quickly after a disaster. *The information technology department has a good system for backing-up servers and databases, and has off-site storage of the back-up tapes. In addition, it is developing the resources necessary to shift processing to one of the juvenile facilities in case of a disaster. However, the Authority has only limited proposed policies concerning business-continuity planning, and no plan.* .... page 15

The Authority isn't in compliance with the a requirement related to business contingency planning. *The Kansas Information Technology Executive Council requires agencies to file a copy of their continuity plans with the Chief Information Technology Officer of the Executive Branch for review, and another copy with the Division of Information Systems and Communication for archiving. Because the Authority has no plan, it hasn't met this filing requirement.* .... page 16

Recommendations .... page 16

APPENDIX A: Scope Statement .... page 17

APPENDIX B: Agency Response .... page 19

This audit was conducted by Allan Foster. If you need any additional information about the audit's findings, please contact Mr. Foster at the Division's offices. Our address is: Legislative Division of Post Audit, 800 SW Jackson Street, Suite 1200, Topeka, Kansas 66612. You also may call us at (785) 296-3792, or contact us via the Internet at LPA@lpa.state.ks.us.

Juvenile Justice Authority Information Systems: Reviewing the Authority's Management of Those Systems

This is the second in a series of specialized compliance and control audits designed to focus on an important area of agency operations that generally hasn't been reviewed—the technical aspects of operating information systems. At the direction of the Legislative Post Audit Committee, this audit focused on the management of the Authority's information systems. Specifically, we reviewed how well the Department secures its information systems. The audit addresses the following questions:

1. **How well is the Juvenile Justice Authority managing the security of its information systems?**

2. **How well is the Authority limiting unauthorized access to its information system resources?**

3. **Is the Authority adequately managing changes to its critical software?**

4. **Has the Authority done adequate disaster-recovery planning to minimize the loss of computer operations in case of a disaster?**

To answer these questions, we reviewed information system standards and best practices in each of the 4 areas listed above, interviewed Authority officials, reviewed and evaluated policies and other documentation, and tested selected computer controls used by the Authority in managing its computer systems.

A copy of the scope statement for this audit approved by the Legislative Post Audit Committee is included in Appendix A. For reporting purposes, we've expanded the scope statement's one question into 4.

The criteria we used in reviewing the Department's management efforts in these 4 areas were from 2 main sources:

- the Control Objectives for Information and Related Technology (COBIT), published by the Information Systems Audit and Control Association
- the Federal Information System Controls Audit Manual, published by the U.S. General Accounting Office.

In conducting this audit, we followed all applicable government auditing standards. In addition, we found some security weaknesses we didn't report for security reasons as required by the Kansas Open Records Act (KSA 45-221 (12). Our findings begin on page 4, following a brief overview.

Overview of the Juvenile Justice Authority's Information Systems Function

The Juvenile Justice Authority was created in 1997 to coordinate and administer custody and programs for juvenile offenders in State custody. The Authority also maintains 4 juvenile correctional facilities across the State. In fulfilling its responsibilities, the Authority handles important confidential information on the juveniles in its custody and supervision.

To handle that information, the Authority has built several networks and computer systems. It has an internal central office network for its 47 FTE employees and networks in each of the 4 juvenile facilities. The Authority also is developing a comprehensive Statewide information system for juvenile offender data that can be accessed by such organizations as juvenile intake and assessment centers, community case management agencies, juvenile intensive supervision providers, and juvenile correctional facilities.

This Statewide data system is called the Juvenile Justice Information System (JJIS). It will consist of the following major applications, most of which will contain sensitive confidential information about juveniles in the Authority's custody and supervision:

- Juvenile Justice Intake and Assessment Management System (JJIAMS)—This system contains **intake and assessment information about all youth who have had contact with a juvenile intake and assessment center.** It has been in operation for over a year, and can be accessed by staff in the judicial districts.
- Community Agency Supervision Information Management System (CASIMS), and the Juvenile Correctional Facilities System (JCFS)—These systems will contain **data on offenders' education programs and medical and mental health treatment programs.** This piece is nearly completed, and several parts of it have been in operation for several months.
- JJA 1600 Placement Screening System—This system contains **information on offenders' placements while in a correctional facility.** It's currently in operation.
- Juvenile Information Folder—This will be a data warehouse for data from each of the other systems to make comprehensive data on offenders available on-line to organizations that deal with offenders. Programming has just begun on this component.

All but one of these are web-based applications to one extent or another. While that makes it easier and more convenient to access juvenile offender data from across the State, it also raises the risk considerably that these data systems may not remain secure.

Currently, the Authority has 7 information systems staff in the central office, and 4 staff at the juvenile facilities. Two of those central office staff have significant security responsibilities—a security officer who also has other management duties, and a full-time security technician. In addition, database security is handled by the database administrator.

Juvenile Justice Authority
AT A GLANCE

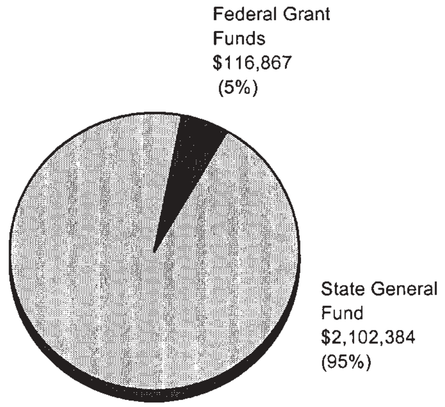
Staffing: The Authority has 11 full-time-equivalent positions in Information Resources, including 4 staff at the State juvenile correctional facilities.

Budget: The Information Resources Section's funding comes primarily from State General Fund appropriations. The Authority also receives moneys from the federal Edward Byrne Memorial Grant for work related to the Juvenile Justice Information System project.

FY 2002 Expenditures

Type	Amount	% of Total
Salaries & Wages	$378,406	17%
Contractual Services	$1,457,674	66%
Commodities	$104,374	5%
Capital Outlay	$148,412	7%
Aid to Local Governments	$130,385	6%
Total Expenses:	**$2,219,251**	**100%**

Sources of Funding for Expenditures



Total Funding: **$2,219,251**

Source: *Juvenile Justice Authority 2003 budget documents*.

Question 1: How Well Is the Juvenile Justice Authority Managing the Security of Its Information Systems?

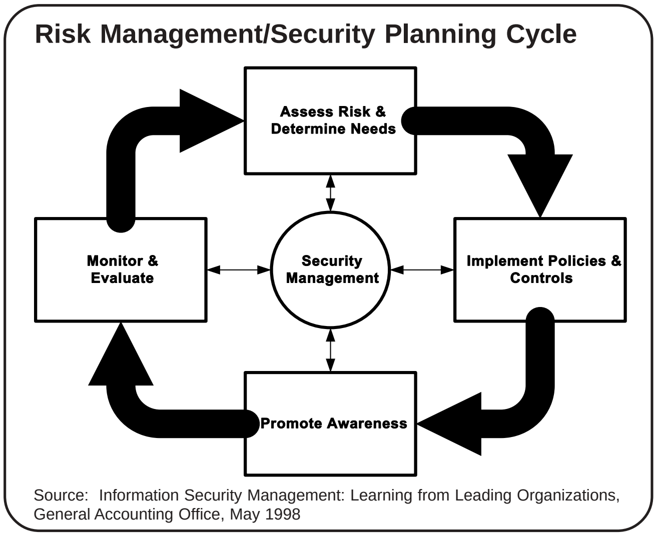
Security planning is a cycle of activity that allows an organization to focus its scarce security resources in the areas that most need them. The Authority has established the foundation of an adequate security function. Two staff have significant security responsibilities, and the function appears to have the support of top management. However, the Authority hasn't conducted a formal risk assessment, the first step in a good security planning process. In examining the Authority's security policies, we also found several areas lacking, such as responding to security incidents, collecting audit trails of actions users take, and considering security in all stages of development of a new computer system. Finally, the Authority hasn't done enough to monitor the effectiveness of its security function. These and other findings are discussed in the sections that follow.

Security Planning Allows an Organization To Identify Its Vulnerabilities and Focus Resources Where They Are Most Needed

Today, information technology is becoming more and more imbedded in business strategies and operations. Likewise, technology is being used more and more to make services more efficient and effective for the public and for State agencies. As a result, keeping information systems and the data in them secure has become an essential function.

Without good security planning, there's an increased risk agencies will have poor security over their information systems, or will focus their security resources in the wrong directions. Security planning should be an on-going cycle of activity. A U.S. General Accounting Office study of the leading non-federal organizations with the most successful security-management functions found that these organizations use 5 common risk-management principles. These are shown in the diagram on the left.

Risk Management/Security Planning Cycle



Source: Information Security Management: Learning from Leading Organizations, General Accounting Office, May 1998

These principles form a cycle of activity that can help organizations ensure their security policies are current and address risks on an ongoing basis. We compared the Authority's security management processes and practices with this list of critical elements.

The Authority Has Never Done A Formal Security Risk Assessment

An organized assessment of risks is the base from which security policies and plans should flow. Identifying these risks helps agencies know where their security systems are most vulnerable. And identifying which risks are most significant helps agencies know where to focus sometimes limited security resources.

The Authority has no policy requiring periodic risk assessments, and has never done a formal assessment. As a result, Authority staff don't know if they are missing important vulnerable areas. For example, the Authority has developed extensive defenses against intruders or virus attacks from outside the agency. However, national statistics show many serious security problems come from an organization's own employees.

The Authority Has Inadequate Security Polices Or Practices in Several Important Areas

Each State agency is required to have a security policy. Its primary purpose is to inform users of their obligations for protecting technology and information assets. Without a policy, security efforts can be haphazard, inconsistent, or ineffective.

We compared the Authority's security policies and practices against the security policy "template" developed by the Department of Administration as a guidance to State agencies, and against other best practices we identified from other sources. The Authority had most of the policies we were looking for, although many weren't written. However, we found several important policies to be missing. The most critical of these are summarized below.

- The Authority was missing policies having to do with incident response and reporting. Such policies establish guidelines for how staff are to respond to various types of security incidents. In theory, they are important so that staff will know what to do in case of a serious security incident (such as cutting off an intrusion immediately, or tracking the intruder long enough to collect the information needed to prosecute the attacker), and who is to do it. Speed is also essential in responding to such an attack in order to protect agency data.

  In this area, we found the Authority was missing policies to:
  - investigate unauthorized access attempts
  - have an incident response plan that details how to respond to intrusions
  - specify the responsibilities of security staff in investigating incidents
  - specify how to report incidents

- The Authority lacked policies on audit trails. Audit trails provide accountability. They allow staff to track important actions—such as successful and unsuccessful log-in attempts, changes to access privileges, and files that have been accessed. Without such audit logs, it is nearly impossible to track what happened during a security incident.

In this area, we found the Authority was missing policies to:

- require audit trails be maintained to track security activity and detect security violations
- specify the minimum events to log
- require periodic review of logs by security staff

We reviewed the logging the Authority does, and found some weaknesses with its approach. We recommended improvements to Authority officials.

- The Authority had no written policies on passwords, and some of its password practices are weak. Passwords are the most commonly used method for controlling computer and data access, but they are also the weakest form of access control. As a result, it's important to have good policies on passwords, and to rigorously enforce those policies. The weakness we found was that it required passwords to be only 5 characters long. The standard is 7 to 8 characters. Fewer characters make it easier for someone to "crack" a person's password and gain unauthorized access to the agency's systems and data. (The Authority does have good policies on the access control requirements for the token system the judicial districts use to access the Juvenile Justice Information System.)

- The Authority's security policies didn't address enforcement issues. Good security policies should specify allowable measures to take against employees who violate the policies.

- The Authority lacked documentation for how some of its servers are configured. Such documentation is important to ensure that any servers that have to be replaced or rebuilt are configured correctly and securely. Mistakes in configuration can often open a server to a hacker.

Since our audit began, the Authority has addressed a number of these weaknesses.

We also noted several less significant security-related problems that still need to be improved. These weaknesses are summarized below:

- The Authority had no policies requiring security to be considered at each stage of a system development project. System development literature shows that security is often added at the end of a software development project, or after a project has been completed. Building in security early in the project results in more secure systems and costs far less. Best practices call for security plans to be developed for all projects under development, and for each phase of system development to include assurances of security and audit controls. Currently, no security staff are involved in the planning stages of the system development process.

- The Authority had no policy for ensuring its security staff get continuing education on an ongoing basis. However, it did send both security staff to security training last year.

- The Authority had no policy on protecting sensitive agency data on laptops. Possible ways to protect such data: keeping it on diskettes or other removable media, or encrypting the documents.

- The Authority is one of the few agencies that has an intrusion detection system, but it had no policy defining how the system was to be used. An intrusion detection system is expensive and complex software that allows agencies to monitor for people trying to break into agency networks.

The Authority Does Little Active Monitoring Of Its Security Function's Effectiveness

Information system security involves a complex set of activities that are continually in flux, and that involve a number of people. Even under the best of circumstances, it's difficult to maintain security at an acceptably high level. The only way for upper-level management to ensure that security policies are carried out and remain effective is to monitor those policies and controls.

The Authority has no policies in this area, and does little active monitoring of how well its security function is working to safeguard its systems and information from intrusion. In reviewing the security configurations of the network operating system, we found instances where important settings were different than the security officer thought they were. Periodic monitoring would uncover such inconsistencies. (We did find certain exceptions: it appeared that the firewalls, the intrusion detection system, and the virus software were actively monitored.)

Conclusion

Two of the policy areas we found to be deficient--assessing risk and monitoring compliance–are 2 of the 5 core activities in the security planning cycle. Without these 2 activities the effectiveness and efficiency of the Authority's security efforts is diminished. When the Juvenile Justice Information System is complete, the Authority will be responsible for protecting the security and integrity of a large amount of data on juveniles, including such sensitive data as medical and mental health histories, treatment program records, and law enforcement records. Some of this data is accessed through a web interface, which makes assess easier but also makes exposure greater. The combination of highly confidential data and exposure to the internet necessitates a dynamic and effective information security program based on sound planning. By incorporating a periodic cycle of risk assessment, policy development, and monitoring of the security function, the Authority could maintain security controls that were current and effective.

Recommendations

1. To ensure that it manages the security of its systems effectively and efficiently, the Juvenile Justice Authority should develop the following written policies:

   a. a risk management policy requiring periodic risk assessments to identify what the Authority's risks are, and where security controls are needed to mitigate those risks

   b. incident response and reporting policies that establish guidelines for how staff are to respond to security incidents

   c. an accountability policy specifying what types of audit trails are to be maintained, and requiring staff to review audit logs regularly

   d. a password policy that includes password requirements which meet best practices

   e. an enforcement policy which specifies how security policies will be enforced

   f. an addition to the system development policies requiring security to be considered in each phase of software development projects

   g. a continuing education policy for security staff to help ensure that staff keep up-to-date on security issues

   h. a laptop security policy requiring sensitive data on laptop computers to be protected

   i. an intrusion detection system policy specifying how the system is to be used

   j. a security monitoring policy to help ensure that security controls and policies address risk areas effectively and that staff comply with security policies

Question 2: How Well Is the Authority Limiting Unauthorized Access To Its Information System Resources?

Access controls are procedures an organization uses to control who is allowed into the system, and what they can do once they're there. In many ways, the Authority has good access controls. It has strong access controls for its Statewide juvenile justice information system databases, and it has intrusion detection systems that allow staff to monitor traffic coming into the networks. However, it also has some significant weaknesses in access controls that put the Authority's central office systems at higher risk, such as inadequate password requirements and not staying current on security patches in important software. Finally, the Authority's method of controlling access to data could be improved by better documenting what users are allowed to access. These and other findings are discussed below.

Access Controls Are the Core of an Organization's Security, Determining Who Gets in and What They're Allowed To Do Once They're There

Access controls protect computer systems and system data from unauthorized modification, disclosure, loss, or impairment. They are designed to limit access only to those people who are authorized, and to limit authorized users to the minimum level of access they need to do their jobs. These controls fall into the following major categories:

- classifying information resources according to their criticality and sensitivity
- maintaining a current list of authorized users, what they're authorized to access, and how much they're allowed to do
- establishing physical and logical controls to prevent or detect unauthorized access
- monitoring access, investigating apparent security violations, and taking appropriate remedial action

The Authority has some access control elements that provide very strong security for agency data. The Authority uses ordinary password controls for its central office network. However, it goes beyond ordinary password controls and uses a method of authenticating users that's far more secure for its web-based Juvenile Justice Information System. That system contains the most confidential data the Authority is responsible for— information about juveniles. To access the server for that system, a user has to:

- type in a random number that matches the one the computer has generated for that user. That number shows up on a small device called a "token" the user carries that's synchronized with the computer. A different random number is generated every minute.
- type in a personal identification (pin) number

The Authority also uses an intrusion detection system. Such systems monitor any traffic attempting to come into the Authority's network. They can alert the security officer about attempts to break into or disrupt the system. Few State agencies have such systems at this time.

Weaknesses in Some of the Access Controls In the Authority's Central Office Network Increased Its Vulnerability

Because network security is extremely complex, it's important for an agency to have good systems to ensure that network access controls are up-to-date and working. We found the Authority generally had good network controls—it made good use of tools that simplify some of the possible complexity in network security, and was good at authorizing users' access only to those resources they needed to do their work. However, we did note the following significant weaknesses:

- The Authority had some weak network passwords requirements. To test the strength of the passwords, we used password cracking software on a sample of users' passwords. We were able to break 27% of the passwords in 2 hours and a total of 70% of the passwords in 8 hours, including some administrative passwords. If someone breaks an administrative password, they essentially can do whatever they want to the computer. The major problems with the passwords: some were too short, some used proper names or dictionary words, and most weren't combinations of numbers, letters, and special characters.

- The security "patches" for the Authority's web-based Juvenile Justice Information System database software weren't current. As new vulnerabilities in software are discovered, software manufacturers release security patches that address them. Not keeping current with these security patches puts an entity's computer system and data at much greater risk. For example, the computer worm that caused an estimated $1 billion damage to computer systems nationwide in January 2003 took advantage of vulnerabilities for which patches had been available since July 2002. The Authority didn't get this worm, but it could have if it hadn't had other controls in place that protected it.

- Although the Authority had a policy to disable accounts immediately after an employee leaves, information systems officials weren't always notified. It's important to delete or disable employees' accounts when they leave an agency so they can no longer access the network We found that 2 of the 10 employees who had left employment in the previous year still had active log-in accounts.

- The intruder lockout function wasn't turned on for the central office and for one of the juvenile facilities. This function—which is designed to prevent someone from being able to repeatedly guess someone else's password—locks an employee's account after a certain number of failed attempts (usually 3) at logging on. We also noted that the token system the Authority used for the web applications allowed a larger number of guesses than was prudent before locking someone out.

- The Authority had set its firewall to give users in 2 segments of the network more access than they needed to other parts of the network. Networks usually are segmented into different sections so it's easier to isolate users and prevent them from accessing parts of the network they don't need to be in. For example, the Authority's central office system is in a different segment of the network from the one that contains the Juvenile Justice Information System data. However, we found that staff had set the Authority's firewall to allow unlimited traffic between those two segments. This unnecessarily opened the central office network to possible access from non-Authority users across the State who access the Juvenile Justice Information System. Officials told us they had done this temporarily to monitor the traffic on the network and to make it easier for information systems staff to administer the servers in the other section of the network.

The Authority's Method Of Assigning Access To Data Could Be Improved

The Authority has a system to make sure new users get assigned access only to those files they need to do their jobs. Supervisors make that determination and submit a form to the information systems manager, who has to approve it. That part of the Authority's system appeared to work well. We found the following problems, however:

- Information systems staff don't retain the original forms used to assign employees' access privileges. That makes it difficult to check to see what access was requested for a particular employee.

- Information systems staff don't periodically review employees' access privileges. As time passes, employees are promoted, change to different departments, or change projects. If no one reviews their access privileges, they could end up with access to far more files than they actually need to do their current jobs.

- The general network diagram the Authority publishes in its annual report provides more information than is prudent. That diagram isn't extremely detailed, but it would be better not to publish it.

- The Authority requires Juvenile Justice Information System users to get criminal background checks, but has given them access even when they didn't pass. We noted that one judicial district had asked for tokens for 3 employees who didn't pass the criminal background check. District officials indicated they'd looked into those employees' histories and approved them for various reasons. The Authority granted access. Although the judicial districts are the owners of the data, the Authority is the custodian of that data. It appeared to us the Authority should do some work of its own to decide whether to grant the access.

Conclusion

Restricting unauthorized access to computer systems is technical and complex. Elements of access controls are included in the network, server, and desktop computer operating systems, databases, applications, and firewalls. Some of the problems we identified in this question were serious mistakes or oversights. At the same time, nearly all are fairly easily resolved and Authority officials already have addressed most of them. However, it's likely that other problems will surface over time. Unless the Authority addresses the monitoring deficiencies cited in question one, it won't know when future problems arise, exposing itself to greater security risks.

Recommendations

1. To ensure that it has adequate controls over access to its computer systems, the Authority should:

   a. develop a policy requiring that security patches for software be tested and applied expeditiously

   b. reduce the number of unsuccessful log-on attempts allowed in the Juvenile Justice Information System before a user's account is locked

   c. develop a system to ensure that the Authority's personnel division immediately notifies the information resources division when employees leave the agency, so that the employee's computer access can be disabled

   d. retain data access forms to document which files each employee is authorized to access, and periodically review employee access authorizations to ensure that the authorizations are current

2. To ensure that confidential data on juveniles are adequately protected, as soon as the Juvenile Justice Information System is complete the Authority should contract with a third-party for a detailed vulnerability assessment or penetration test of the system.

Question 3: Is the Authority Adequately Managing Changes to Its Critical Software?

The Authority recently developed a process to manage changes that had most of the steps we were looking for, but that process is missing some important elements and it needs to be more thoroughly documented. The most significant problems we noted: there was no requirement for management approval of changes being made to the production software, and there was no formal process for tracking and documenting changes to the server and network software. The Authority also needs to develop a more organized system of tracking changes throughout the process. These findings are summarized in the sections that follow.

Because of the Dynamic Nature of Computer Software, It's Important To Have a Well Organized System To Manage the Process of Making Changes

In many ways, software is delicate and difficult to maintain. A large and complex computer program—such as the one the Authority is in the process of developing—is constantly in flux. Something always needs to be changed or corrected as new functions have to be added, bugs are discovered, laws or regulations change, or the system is made easier or more efficient to use. As a result, computer programs remain works in progress long after they are put into daily use.

If the activities involved in changing software aren't closely organized and managed, the software can quickly become unreliable. Managing changes in software is called "change control." Among the best practices for change control are the following:

- using a formal process, such as a change control committee, to review change requests
- categorizing and prioritizing requested changes
- documenting change requests in writing
- documenting authorization of changes
- analyzing the technical and security impact of a requested change prior to approval
- using a formal tracking system to control changes
- requiring documented management approval before changes are put into production

The Authority's change control process had many of the elements of a good system, but several improvements are needed. Although the Authority's change control practices cover most of the 18 elements of best practice we were looking, its written policies only address 6 of those elements. We also noted the Authority was missing change control processes in the following areas:

- the Authority doesn't have a formal "configuration management process" that would document changes to the network and server software.

- the Authority doesn't require the information technology manager to approve in writing the incorporation of software changes into the production software. This approval process would reduce the risk of a programmer inserting untested or poorly tested modifications into the production software. Also, it would give the Authority a change-control log documenting each change instituted in the production software.

- the Authority doesn't use the change control process for tracking computer bugs. Those bugs are simply given to the programmer to fix.

Finally, we noted the Authority needs to develop a better tracking form and to require management to document completion of important steps. When we reviewed the one change that had gone through the process, it was difficult to determine from the current tracking form when and whether the following had happened: programming was completed, user acceptance testing was completed, new codes were moved into production, the documentation was updated, and users were notified of changes. If all steps aren't included on the tracking form some could be overlooked, especially when numerous changes are in process at the same time.

Recommendation

1. To ensure adequate management of the maintenance and updating of its software, the Authority should:

   a. expand its written change control policies to address best practices, including policies requiring:

   - a configuration management system be used to track changes to network and server software
   - a manager to approve, in writing, all movements of software changes into the production software
   - the process to be applied to system "bugs"

   b. develop a tracking form or database which would show steps in the change control process and document completion of each step for all changes.

Question 4: Has the Authority Done Adequate Disaster-Recovery Planning To Minimize the Loss of Computer Operations in Case of a Disaster?

Business continuity planning addresses an organization's ability to continue functioning when normal operations are disrupted. The Department hasn't done any business-continuity planning, increasing the risk it won't be able to respond in the event of a disaster.

An Organization Needs Good Business Continuity Planning In Order To Quickly Recover Critical Operations After A Disaster

Business continuity planning addresses an organization's ability to continue functioning when normal operations are disrupted. By necessity, it includes planning for contingencies and is focused on the information system functions that are the most critical to continue agency operations. Often this is called disaster-recovery planning.

Good business continuity planning involves the following:

- developing a written continuity plan that is in line with the agency's objectives
- testing the plan and keeping it up-to-date
- making sure each employee knows their responsibilities as specified in the plan
- establishing adequate off-site storage for critical backup tapes
- developing alternative processing procedures for user departments to implement until processing can be restored

The continuity plan itself discusses the most likely types of disasters and specifies detailed steps to take to recover services, including assigning specific roles and responsibilities to specific staff members.

The Authority Lacks the Tools Necessary To Recover Operations Quickly After a Disaster

Officials told us they had started to do some business-continuity planning forY2K, but the effort never got very far. We found that the information technology department does have a good system for backing-up servers and databases, and has off-site storage of the back-up tapes. In addition, it has started developing the resources to shift some processing to one of the correctional facilities in case of a disaster. The only policy the Authority has in this area is a proposed policy that would require all agencies that provide recordkeeping for the Juvenile Justice Information system to develop a disaster recovery plan and test it. However, the Authority itself has made no recent efforts to conduct planning, and the Authority has no business continuity plan.

Without a plan, the Authority's staff would have access to back-up data if a disaster affected the central office, but they would have no action plan to let employees know what equipment, software, or supplies they needed to collect, where they should go, or what they should do.

The Authority Isn't in Compliance with the Information Technology Executive Council Policy On Business Contingency Planning

The Kansas Information Technology Executive Council is responsible for adopting information technology policies and procedures for all State agencies. The Council has a policy on contingency planning (Policy 3210) that's very similar to the COBIT standards. The policy requires agencies to file a copy of their continuity plans with the Chief Information Technology Officer of the Executive Branch for review, and another copy with the Division of Information Systems and Communication for archiving. The Authority hasn't complied with that policy.

Recommendations

1. To help ensure that it can continue functioning when normal operations are disrupted by a disaster, the Authority should approve policies requiring it to conduct business continuity planning, which would include the following:

   a. a risk analysis that assesses the most likely disaster scenarios

   b. a disaster recovery plan that addresses the most likely disasters that might befall the Authority. This plan should assign roles and responsibilities to specific staff, and present specific steps for staff to follow in recovering computer operations.

   c. arrangements that allow the Authority to continue offering computer services in case the central office computers aren't available for a period of time. This could include having redundant servers at one of the juvenile facilities or contracting with a vendor that offers off-site computing capability.

   d. training staff in how to use the plan in the event of an emergency

   e. conducting periodic testing of the disaster recovery plan

2. The Department should come into compliance with the requirements of the Information Technology Executive Council's policy on contingency planning.

APPENDIX A

Scope Statement

This appendix contains the scope statement for this audit. This scope statement is being used in a series of compliance and control audits of agency information systems approved by the Legislative Post Audit Committee on December 3, 2001.

SCOPE STATEMENT

Juvenile Justice Authority Information Systems: Reviewing the Authority's Management of Those Systems

In fiscal year 2001, the Juvenile Justice Authority spent about $690,000 on its information systems. In all, 11 staff control information systems for the Authority and the 4 juvenile correctional facilities. The Department has been developing software for the planned juvenile justice information system and is expected to complete that project next year.

During the last few years, concerns have been expressed about the lack of monitoring of State computer systems. Each year State agencies become more dependent on their computer systems and on the data those systems contain to make decisions and fulfill their missions. More and more, computing is moving out of the data center and into the hands of staff who use the data to make decisions. Computers and computer networks also are being used to communicate with the public, provide services, and conduct business.

These are positive developments that can result in increased efficiency and effectiveness and better service. However, significant risks are associated with these advances in technology that agencies should be addressing and managing. At present there is little oversight of agencies' computer operations to monitor whether these risks are being adequately managed.

To help address these risks, the Legislative Post Audit Committee approved information system audits to be done as an adjunct to the Division's compliance and control audits. The second of these audits looks at the Juvenile Justice Authority's information systems, and will address the following question:

1. **Is the Juvenile Justice Authority managing its information systems in a manner that reduces the risk of loss due to errors, fraud, or other illegal acts and disasters?** To answer this question, we will review the Authority's policies and practices in the following areas:

    - **Security Planning and Management**–We would review the agency's system of managing its information system security, with emphasis on security policies and procedures.
    - **Access Control**–We would review how the agency protects its information system resources against unauthorized access. This would include examining both physical and logical security controls.
    - **Change Control**–We would review how agency staff manage the maintenance and updating of important software.
    - **Business Continuity**–We would review the agency's plans for how the staff would continue to operate in situations such as power outages and other disasters, and whether they adequately test those plans. This would include a review of the agency's policies for backing-up computerized data.

APPENDIX B

Agency Response

On March 5, 2003, we provided copies of the draft audit report to the Juvenile Justice Authority. Its response is included in this appendix.

KANSAS

JUVENILE JUSTICE AUTHORITY

DENISE L. EVERHART
ACTING COMMISSIONER

KATHLEEN SEBELIUS, GOVERNOR

March 12, 2003

Ms. Barbara Hinton, Legislative Post Auditor
Legislative Division of Post Audit, Mercantile Bank Tower
800 SW Jackson Street Suite 1200
Topeka, KS 66612-2212

Dear Ms. Hinton:

Thank you for the opportunity to review and respond to the findings and recommendations made in the performance audit, "Juvenile Justice Authority Information Systems: Reviewing the Authority and Management of Those Systems."

The Juvenile Justice Authority (JJA) respects and appreciates the extensive analysis and recognizes the importance of information systems security.

Please see our attached detailed response, and again, thank you for the opportunity to utilize the audit process to improve our system security.

Sincerely,

Denise L. Everhart
Acting Commissioner

DLE:bt

KANSAS

DENISE L. EVERHART
ACTING COMMISSIONER

JUVENILE JUSTICE AUTHORITY

KATHLEEN SEBELIUS, GOVERNOR

JUVENILE JUSTICE AUTHORITY INFORMATION SYSTEMS
RESPONSE TO LEGISLATIVE POST AUDIT
MARCH 2003

Question 1: How Well IS the Juvenile Justice Authority Managing the Security of Its Information Systems?

Recommendations

1. To ensure that it manages the security of its systems effectively and efficiently, the Juvenile Justice Authority should develop the following written policies:

a. a risk management policy requiring periodic risk assessments to identify what the Authority's risks are, and where security controls are needed to mitigate those risks

Response: An internal IT risk management policy will be created. The policy will include all areas identified.

b. incident response and reporting policies that establish guidelines for how staff are to respond to security incidents

Response: We had a rough draft of a policy started at the time of the audit. This process will continue and the formal policy completed.

c. an accountability policy specifying what types of audit trails are to be maintained, and requiring staff to review audit logs regularly

Response: An internal IT policy will be created and be based on the recommendations outlined in the audit.

d. a password policy that includes password requirements which meet best practices

Response: A policy is currently in the approval process addressing this recommendation.

e. an enforcement policy which specifies how security policies will be enforced

Response: A policy(s) that addresses policy enforcement will be created.

f. an addition to the system development policies requiring security to be considered in each phase of software development projects

Response: A review of current policy and practice will be done and address the implementation of security as recommended.

g. a continuing education policy for security staff to help ensure that staff keep up-to-date on security issues

Response: A review of the current continuing education and training policy will be done and revised to meet this recommendation. The ability to comply with this recommendation is contingent upon adequate funding.

h. a laptop security policy requiring sensitive data on laptop computers to be protected

Response: A policy will be written to increase the security of laptops beyond what is currently required.

i. an intrusion detection system policy specifying how the system is to be used

Response: An internal IT policy will be created and be based on the recommendations outlined in the audit.

j. a security monitoring policy to help ensure that security controls and policies address risk areas effectively and that staff comply with security policies

Response: An internal IT policy will be created to address security monitoring.

Question 2: How Well Is the Authority Limiting Unauthorized Access To Its Information System Resources?

Recommendations

1. To ensure that it has adequate controls over access to its computer systems, the Authority should:

a. develop a policy requiring that security patches for software be tested and applied expeditiously

Response: An internal IT policy will be created to ensure that the organization is implementing patches and upgrades consistently.

b. reduce the number of unsuccessful log-on attempts allowed in the Juvenile Justice Information System before a user's account is locked

Response: We have already addressed this recommendation.

c. develop a system to ensure that the Authority's personnel division immediately notifies the information resources division when employees leave the agency, so that the employee's computer access can be disabled

Response: There is a draft policy created by the IT division that addresses this recommendation and is currently under review by the personnel division. The policy will be processed and adopted by the agency.

d. retain data access forms to document which files each employee is authorized to access, and periodically review employee access authorizations to ensure that the authorizations are current

Response: The IT division will retain a copy of all data access forms. There will be a periodical review of data access levels to ensure they are appropriate.

2. To ensure that confidential data on juveniles are adequately protected, as soon as the Juvenile Justice Information System is complete the Authority should contract with a third-party for a detailed vulnerability assessment or penetration test of the system.

Response: We agree that the protection of the juvenile information is of high concern and that a vulnerability assessment and a penetration test would be helpful to ensure current processes are adequate. We have currently worked with outside experts to ensure our current design is solid but confirmation of the implementation would be helpful. These tests done by a third party could be expensive. The agency will address this issue as funding and resources allow.

Question 3: Is the Authority Adequately Managing Changes to Its Critical Software?

Recommendation

3. To ensure adequate management of the maintenance and updating of its software, the Authority should:

a. expand its written change control policies to address best practices, including policies requiring:

- ***a configuration management system be used to track changes to network and server software***
- ***a manager to approve, in writing, all movements of software changes into the production software***
- ***the process to be applied to system "bugs"***

Response: The agency will address recommendations and expand the current policy to meet the agencies business requirements.

b. develop a tracking form or database which would show steps in the change control process and document completion of each step for all changes

Response: This recommendation will be addressed when the agency expands the current policy as noted above.

Question 4: Has the Authority Done Adequate Disaster-Recovery Planning To Minimize the Loss of Computer Operations in Case of a Disaster?

Recommendations

4. To help ensure that it can continue functioning when normal operations are disrupted by a disaster, the Authority should approve policies requiring it to conduct business continuity planning, which would include the following:

a. a risk analysis that assesses the most likely disaster scenarios

b. a disaster recovery plan that addresses the most likely disasters that might befall the Authority. This plan should assign roles and responsibilities to specific staff, and present specific steps for staff to follow in recovering computer operations.

c. arrangements that allow the Authority to continue offering computer services in case the central office computers aren't available for a period of time. This could include having redundant servers at one of the juvenile facilities or contracting with a vendor that offers off-site computing capability.

d. training staff in how to use the plan in the event of an emergency

e. conducting periodic testing of the disaster recovery plan

Response: This recommendation was identified in the agency's three year Information Technology Management and Budget Plan turned in to the KITO office in September and published January 2003. This extensive project involves all aspects and levels of JJA. The agency will complete the process and develop a comprehensive plan that addresses the recommendations.

5. ***The Department should come into compliance with the requirements of the Information Technology Executive Council's policy on contingency planning.***

Response: A statement of completion will be forwarded to the Information Technology Executive Council when the plan is done. Due to security requirements of the agency we do not intend to release the document outside of the agency, approval could be made to review the plan for compliance and content.